Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.445 – 451

SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS IN CLOUD COMPUTING USING SHA-1

Prof. J.Nulyn Punitha[1], M.Tamilarasi[2]
Department Of Computer Science and Engineering, IFET College of Engineering, Villupuram-605602, India
mailnulyn@gmail.com
tamilaarsimg@gmail.com

ABSTRACT: Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHRs, we leverage (SHA-1) techniques towe propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. encrypt each patient's PHR file. Different from previous works in secure data outsourcing,focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority SHA-1Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme. A high degree of patientprivacy is guaranteed simultaneously by exploiting multiauthority SHA-1. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

I. INTRODUCTION

The cloud computing which is a recently evolved metaphor based on utility of the computing resources, it involves the deployment of remote servers and software networks which allows centralized data storage and also online access to remote services and networks. The m-healthcare is the abbreviation of mobile healthcare, the term which is used in providing treatment for the patients online and also supported by mobile devices. The m-healthcare field has now been emerging as a segment of e-health care. The m-healthcare makes the maximum usage of the information

and communication technology which includes the communication satellite, PC's, mobile phones etc., in order to provide health services and information. The m-healthcare applications involves the collecting of community and clinical health data using the mobile devices. It also involves the delivery of healthcare information to patients, practitioners and researchers. It is also used in real-time monitoring of patient for diagnosis, and direct provision of care. The m-healthcare mobile social network has nowadays emerged as a reassuring next-generation healthcare system which is increasingly adopted by the US and European governments. With the rapid development of sensor and wireless communication Technologies the m-healthcare can help patients better manage their health related activities. It helps to maintain the personal health information records – suchas the immunization records, laboratory results, screening due date etc. By maintaining the records in electronic form makes it easier for the patients to update the records and also share the same. When the patient is provided with a facility of tracking the personal health information and have the health information tools to manage their health, they become more informed about the health and healthcare information moreover it promotes better health care by enabling the patients manage the personal health information from various providers which improves the synchronization. Online m-healthcare can also ensures that the patients' information is made available in case of an emergencies and also when the patients are traveling.

The enhanced multilevel privacy preserving m-healthcare brings in a direct and secure communication between the patients and healthcare providers. It also make the process of communicating with the patients faster and easier. This paper proposes a methodology in which, the patients can be informed prior in case a health

II. Related Work

Distributed sensor data storage and retrieval have gained increasing popularity in recent years for supporting various applications. While distributed architecture enjoys a more robust and fault-tolerant wireless sensor network (WSN), such architecture also poses a number of security challenges especially when applied in mission-critical applications such as battlefield and e-healthcare. First, as sensor data are stored and maintained by individual sensors and unattended sensors are easily subject to strong attacks such as physical compromise, it is significantly harder to ensure data security. Second, in many mission-critical applications, fine-grained data access control is a must as illegal access to the sensitive data may cause disastrous results and/or be prohibited by the law. Last but not least, sensor nodes usually are resource-constrained, which limits the direct adoption of expensive cryptographic primitives.

Most of the current trust models in peer-to-peer (P2P) systems are identity based, which means that in order for one peer to trust another, it needs to know the other peer's identity. Hence, there exists an inherent tradeoff between trust and anonymity. To the best of our knowledge, there is currently no P2P protocol that provides complete mutual anonymity as well as authentication and trust management. We propose a zero-knowledge authentication scheme called pseudo trust (PT), where each peer, instead of using its real identity, generates an unforgeable and verifiable pseudonym using a one-way hash function.

(2)Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control(3). for data access control to PHRs stored in semitrusted servers.

III. Proposed Work

In distributed m-healthcare cloud computing systems, all the members can be classified into three categories:

The directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information. Verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes. Achieving data confidentiality and identity privacy with high efficiency.

- User Counseling
- Access Control

- Security Analysis
- Distributed Cloud Computing
- Overall Report

1. User Counseling

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

Each data owner (e.g., patient) is a trusted authority of her own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD. Since the users are personally known by the PHR owner, to realize patient-centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. For PSD, *data attributes* are defined which refer to the intrinsic properties of the PHR data, such as the category of a PHR file. For the purpose of PSD access, each PHR file is labelled with its data attributes, while the key size is only linear with the number of file categories a user can access.

2. Access Control

In distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and verify the patient's identityand the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes (i.e. since they are not authorized by the patients, we use the term 'indirectly authorized' instead). They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained. Byextending the techniques of attribute based access control and designated verifier signatures on de-identified health information, we realize three different levels of privacy-preserving requirement mentioned above.

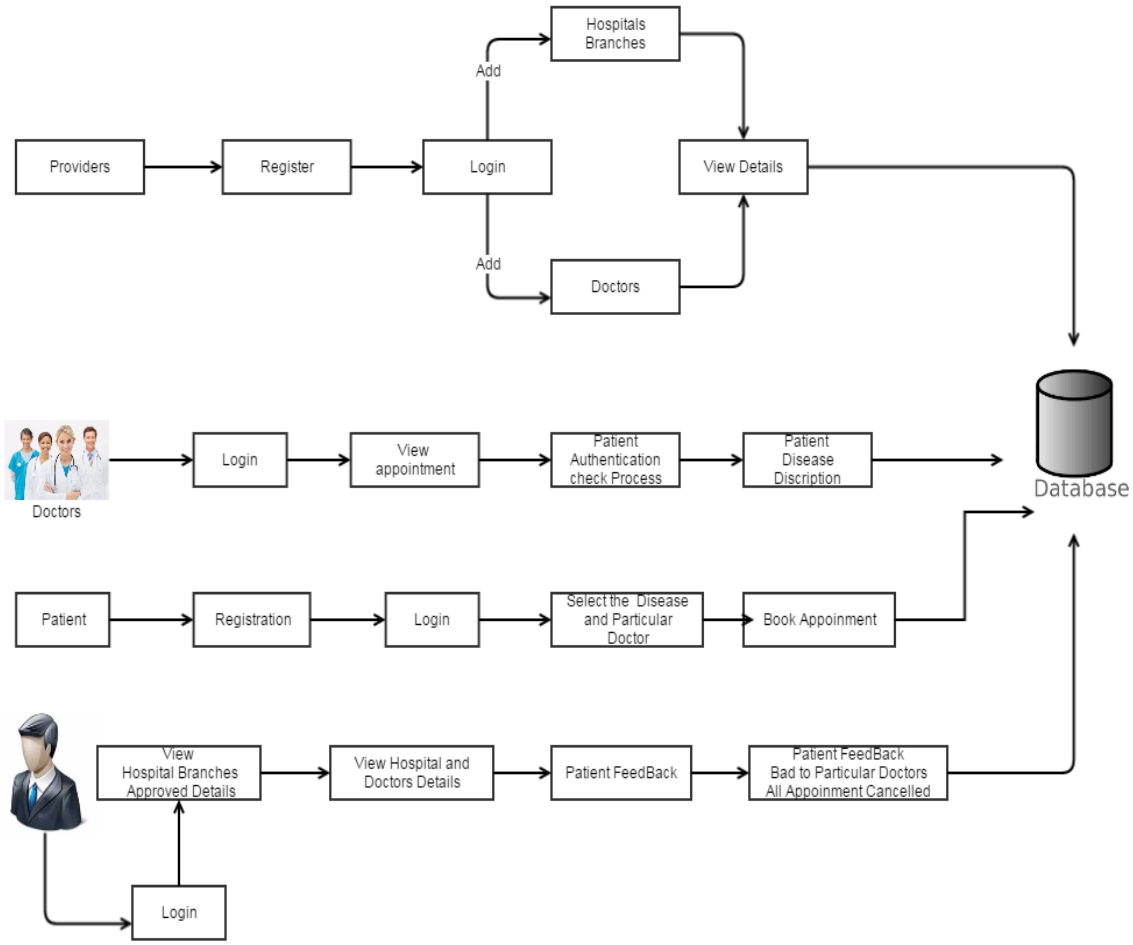
3. Security Analysis

The security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying GBDH problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios in More significantly, without the knowledge of which physician in the healthcare provider is professional in treating hisillness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfies the access policy can recover the PHI and the access control management also becomes more efficient.

4. Distributed Cloud Computing

We consider the server to be semi-trusted, That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

Architecture:



5. **M-Healthcare System**

We propose a patient self-controllable and multilevel privacy-preserving cooperative authentication scheme (PSMPA) based on ADVS to realize three levels of security and privacy requirement in distributed m-healthcarecloudcomputing system which mainly consists of the following five algorithms: Setup, Key Extraction, Sign, Verify and Transcript Simulation Generation.

IV. Experimental Results

Tables are created dynamically to meet the requirements on demand. Reports, as it is obvious, carry the gist of the whole information that flows across the institution.

This application must be able to produce output at different modules for different inputs.

Register:

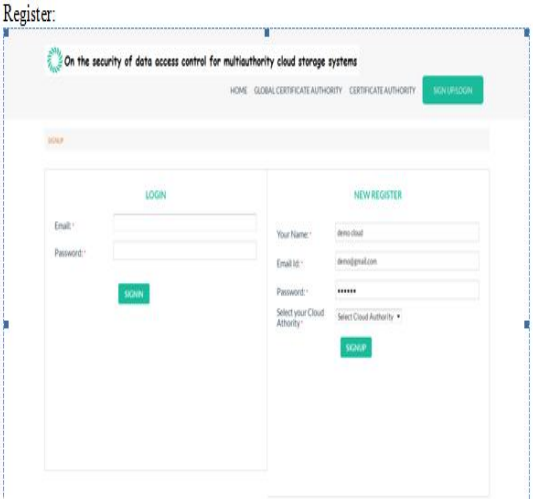


Fig 1:register.

Login:

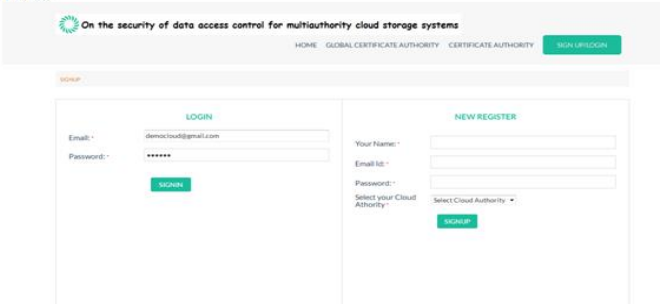


Fig 2: Login

Fileupload:

Fig 3:fileupload

Fig 4:patient list

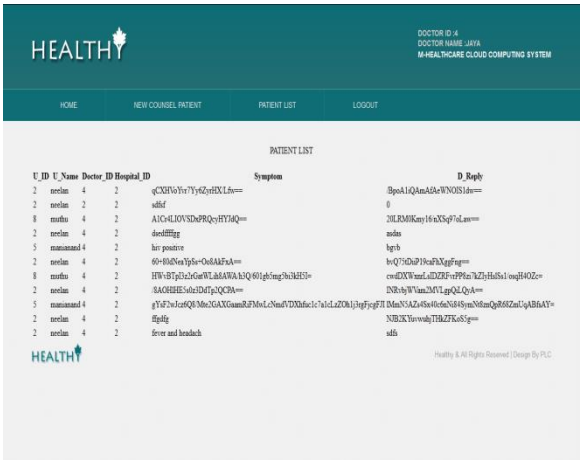


Fig 5:Admin overall report

V. Conclusion

In this paper, a method of Patient personal health record encrypted are proposed, the formal security proof and efficiency evaluation which illustrate our psmpa can resist various kinds of malicious attacks and far out performs previous scheme in terms of storage, computational and communication over head.

References

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, *Stud. Comput.Intell.*Springer-Verlag, 2010, vol. 278.

[2] I. Iakovidis, Towards Personal Health Record:CurrentSutuation, Obstracles and Trends in Implementation of Electronic Healthcare Records in Europe, International Journal of Medical informatics,52(1):105-115,1998.

[3] S.YU, K. Ren and W. Lou, FDAC:Towards Fine grained Distributed Data Acess Control in Wireless Sensor Networks, in IEEE INFOCOM 2009.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670,2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Modelfor Information Retrieval in Wireless Sensor Networks Using EnhancedAPTEEN Protocol," *IEEE Trans. Parallel Distrib.Syst.*, vol. 13, pp.1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," *Comput.Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, pp. 23–28, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a*et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp.2882–2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc.IEEE NCA*, 2007, pp. 145–152.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in *Proc. WiCOM*, 2008, pp. 1–5.

